⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭64－73449

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和64年(1989)3月17日
G 06 F 15/00		7361－5B	
9/06	330	B－7361－5B	

審査請求　未請求　発明の数 1　（全5頁）

⑤4発明の名称　暗証番号入力方式

⑳特　願　昭62－230851
㉒出　願　昭62(1987)9月14日

⑦2発明者　宍道　徹夫　茨城県日立市大みか町5丁目2番1号　株式会社日立コートロールシステムズ内
⑦1出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
⑦1出願人　株式会社日立コントロールシステムズ　茨城県日立市大みか町5丁目2番1号
⑦4代理人　弁理士　鵜沼　辰之　外1名

明　細　書

1．発明の名称

暗証番号入力方式

2．特許請求の範囲

1．データを入力し、該データに基づく出力を表示する端末と、該端末よりの前記データにより、所定の判断、所定の出力を行う演算手段と、乱数を発生し該演算手段に出力する乱数発生手段と、データ加工ルールを格納し該演算手段に出力するルール格納手段と、前記データを記憶し該演算手段に出力する記憶手段とからなり、前記端末への特定操作により、前記演算手段は、該特定操作に基づく情報を前記記憶手段に記憶させると共に前記乱数発生手段に乱数を発生させ、該乱数を前記端末に表示して前記情報に対応した前記データ加工ルールにより前記乱数の加工を要求し、この要求により前記端末に入力された第1加工データと、前記記憶手段に記憶された前記情報により前記ルール格納手段から該情報に対応したデータ加工ルールを入力して前記乱数を加工して第2加工データを作成し、前記第1加工データと該第2加工データとを比較して一致した場合前記第1データを正しい暗証番号と判断することを特徴とする暗証番号入力方式。

2．前記特定操作に基づく情報が、業務の識別記号であることを特徴とする特許請求の範囲第1項記載の方式。

3．前記特定操作に基づく情報が、所定の前記端末に対する起動操作であることを特徴とする特許請求の範囲第1項記載の方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、暗証番号入力方式に係り、特に端末を使用する際、特定の許可された人物であることを確認するための暗証番号入力方式に関する。

〔従来の技術〕

従来例の1つは、特開昭61－128368号に記載のように、端末から入力するときのキーの配列を暗証番号を入力するたびに変化させることにより、

他人から操作しているキーの位置を見られても、暗証番号そのものは覚えられないようにしていた。

しかし、キーの配置は変化するが、キーそのものは一定であり、入力しているキー（すなわち、「3とか5の数字）を他人に見られると、その時点で暗証番号を盗まれることになるという欠点があった。

従来例の他の1つは、特開昭61－157975号に開示されており、予め登録されている暗証番号に1桁ないしはそれ以上の桁数の暗証番号を追加する方式であるが、この追加された暗証番号は、入力する日付のデータの一部（例えば、日にちの1桁目）を使用することにより、もし入力している暗証番号を他人に見られても、この暗証番号は別の日には無効になるというものである。しかし、日付データから追加の暗証番号を決めているために、同一の日にはこの暗証番号が悪用できるという欠点をもつ。

〔発明が解決しようとする問題点〕

上記のように、従来技術は、他人に端末入力操作を見られたときは、完全に暗証番号の機密性を保持することができなかった。

本発明は、入力している暗証番号そのものを見られても、他人に悪用されることを防ぐ暗証番号入力システムを提供することにある。

〔問題点を解決するための手段〕

上記問題点は、データを入力し、該データに基づく出力を表示する端末と、該端末よりの前記データにより、所定の判断，所定の出力を行う演算手段と、乱数を発生し該演算手段に出力する乱数発生手段と、データ格納ルールを格納し該演算手段に出力するルール格納手段と、前記データを記憶し該演算手段に出力する記憶手段とからなり、前記端末への特定操作により、前記演算手段は、該特定操作に基づく情報を前記記憶手段に記憶させるとともに、前記乱数発生手段に乱数を発生させ、該乱数を前記端末に表示して前記情報に対応した前記データ加工ルールにより前記乱数の加工を要求し、この要求により前記端末に入力された第1加工データと、前記記憶手段に記憶された前記情報により前記ルール格納手段から該情報に対応したデータ加工ルールを入力して前記乱数を加工して第2加工データを作成し、前記第1加工データと該第2加工データとを比較して一致した場合、前記第1加工データを正しい暗証番号と判断する暗証番号入力方式により解決される。

〔作用〕

予め、データ加工ルールを知っている操作者が端末に特定操作を行うと、演算手段は、該特定操作に基づく情報を記憶手段に記憶させるとともに、乱数発生手段に対して乱数を発生させ、この乱数を前記端末に表示して、操作者に対し前記情報と対応した予め知っているデータ加工ルールと前記乱数とから第1加工データを作成して端末に入力することを要求し、前記記憶手段に記憶された前記情報に対応したデータ加工ルールを、ルール格納手段から入力して前記第2加工データを作成し、該第2加工データを前記第1加工データとを比較して一致した場合、前記第1加工データを正しい暗証番号と判断する。

〔実施例〕

以下、本発明の第1実施例を、第1図～第3図により説明する。

第1図は第1実施例の暗証番号入力システムのブロック図を示す。

計算機1の端末2よりデータ入力あるいは問合わせ等を行う際、オペレータが端末操作、すなわちこれから行おうとする業務の認識記号（以下、業務ＩＤと称す）を入力する。計算機1の中の演算処理装置3は、端末入出力装置4を経由して、この業務ＩＤを取り込み記憶装置7に格納し、端末2に「暗証番号を入力して下さい」のメッセージを出力する。この際、乱数発生ルーチン6により無作為の英数字列を作成して端末2に表示すると同時に、記憶装置7に格納する。オペレータは、予め知らされている加工ルールにより表示された英数字列を加工し、その結果を暗証番号として端末2から入力する。演算処理装置3は、この暗証番号を端末入出力装置経由で取り込む。すでに入力されている業務ＩＤを記憶装置7から取り出し、

これに対応する加工ルールを、ルール格納ファイル５から選び出す。また、記憶装置７からすでに端末に表示されている英数字列を取り出し、業務ＩＤに対応する加工ルールにより加工する。加工の具体例としては、加工ルールごとのサブルーチンを準備し、業務ＩＤとそれに対応する加工サブルーチン群を、ルール格納ファイル５に収納しておく。

演算処理装置３は、取り出した英数字列を業務ＩＤに対応する加工サブルーチンに渡し、このサブルーチンにて所定のルールにより英数字列を加工する。この結果と、入力された暗証番号を演算処理装置３にて照合し、一致すれば以降の処理に入り、一致しなければ暗証番号不適切ということで、処理を打ち切る。以上の処理を、第２図の流れ図に示す。第３図を用いて、乱数発生ルーチンにて作成された英数字列と、加工ルールの例を説明する。

業務ＩＤ８である２０を入力した例を示す。計算機より毎回変わる数字列９（この例の場合、５９３１）が表示される。オペレータは、予め加工ルール「１０００の位と１の位の差の絶対値を数字列の各桁の数字にそれぞれ加える。加えた結果が１０を越えたときには、その１桁目の数字を使う」を知っており、この例の場合９３７５を入力する。もし、この入力した数字を第三者に見られても、その人間が同じ業務ＩＤで端末操作したときには、今度は５９３１とは異なる値、例えば、０７４２が表示されるため、正しい暗証番号は２９６４となり、９３７５ではエラーとなる。

次に、第２実施例を第４図，第５図により説明する。第１実施例では、初めに業務ＩＤを端末２から入力し、この業務ＩＤに対応する加工ルールにより暗証番号を決定しているが、入力する端末２により加工ルールを定めることも可能である。すなわち、オペレータが端末２に向つて所定のシステム起動操作、例えばＬＯＧＩＮを行つたところで英数字列を表示して、暗証番号入力をうながす。オペレータは、端末２に対応した加工ルールにより暗証番号を決定し、これを入力する。計算機は、入力された端末番号から加工ルールを選び出し、暗証番号が正しいかどうか確認する。

また、銀行の現金引き出し装置のように使用される業務がすべて同じであり、また位置の端末からの入力を許すような場合は、暗証番号に固定部と可変部を設けることにより、本発明が実施できる。

第４図は、暗証番号に固定部と可変部を設けた第３実施例を示す図である。

利用者が端末２の操作を始めると、まず、「暗証番号を入力して下さい」というメッセージが端末に表示される。このメッセージに引き続いて、乱数発生ルーチンにより作られた無作為の英数字列が表示される。

ここで、利用者は端末から暗証番号を入力することになるが、暗証番号は第４図の例に示すごとく、固定部１３と可変部１４とからなる。第４図の例では、５Ｈ３，０７９がそれぞれ固定部１３である。固定部１３の暗証番号と可変部１４を作り出すための加工ルールは一義的に対応しており、これは予め利用者だけに知らされている。

利用者は、暗証番号の固定部１３をまず入力し、その後引き続いて可変部１４を、表示された英数字列１１と加工ルールから決定し入力する。加工ルールは、例えば、第４図の暗証番号例２の場合固定部１３が５Ｈ３のときには、「表示された数字列の最上位の値を、下位４桁の数字にそれぞれ加えた４桁の数字列」となつているとする。表示された数字列１１の最上位の値は１であり、下位４桁の数字は４４６２であることから、４４６２の各桁の数字に１を加えた５５７３がこの場合の正しい数字列となる。

利用者が固定部５Ｈ３に続いて可変部５５７３を入力すると、コンピュータはすでに表示した英数字列と、入力された暗証番号の固定部１３から加工ルールを選び出し、加工ルールにより可変部１４の値を算出、この値と入力された可変部１４の暗証番号を照合することにより、正しい利用者であるかどうか判断する。

第５図に、この一連の流れを示す。第４図の暗

証番号の例２では、固定部１３の値が０、７９であり、これに対応する加工ルールは、「表示された数字列の最下位から２番目の値を上位４桁の数字からそれぞれ減算した４桁の数字列、ただし減算するとマイナスの値となる場合には、１０をたす」とする。第４図にて表示される数字列１１は、1384462 であるため、最下位から２番目の値は６となり、上位４桁の数字は１３８４となる。各桁より６を減算し、マイナスになつたときには１０を加えると、得られる数字は５７２８となる。

万一、５Ｈ３５５７３あるいは0795728 の暗証番号を入力しているところを他人に見られても、この暗証番号はコンピュータから表示された英数字列1384462 に対応しているものであり、この英数字列は暗証番号を入力するたびに無作為されるため、同じ英数字列が表示される確率は極めて低く、一度見られた暗証番号を悪用されることを防止できる。

〔発明の効果〕

本発明によれば、データ加工ルールを予め操作者と記憶装置に記憶しておき、操作者が端末に特定操作を行うと、その特定操作に基づく情報により、演算手段は乱数を発生し表示して、操作者にその乱数と予め知つているデータ加工ルールから第１加工データを作成させて入力させ、一方、前記情報に対応したデータ加工ルールと前記乱数とにより第２加工データを作成し、この第２加工データと第１加工データとを比較して一致した場合、第１加工データを正しい暗証番号と判断するので、入力している暗証番号そのものを他人に見られても、データ加工ルールを知らないこの他人は、この番号を暗証番号として使用することができないという優れた効果がある。

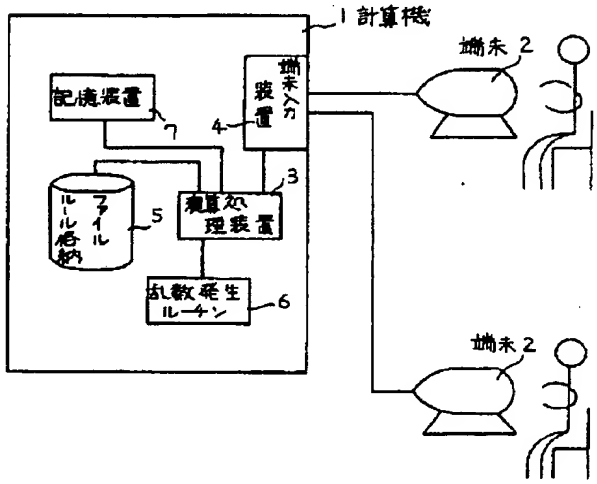
４．図面の簡単な説明

第１図は本発明のシステムブロック図、第２図は暗証番号を処理する流れを示す図、第３図は暗証番号加工ルールの例を示す図、第４図は暗証番号に固定部と可変部とを設けた実施例を示す図、第５図は第４図の処理の流れを示す図である。

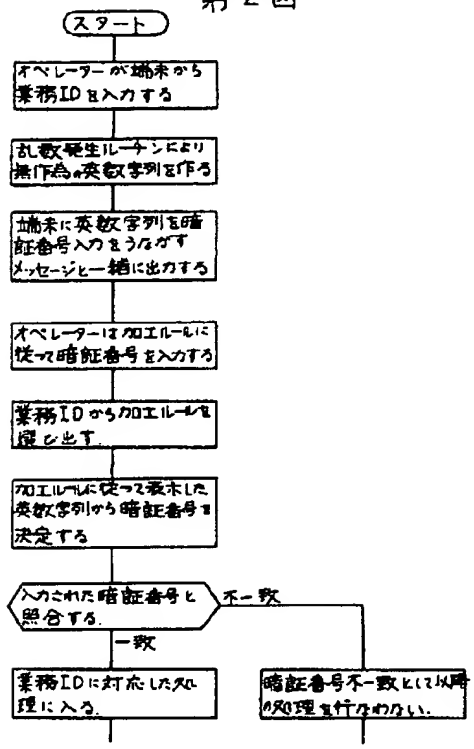
１…計算機、２…端末、３…演算処理装置、４…端末入出力装置、５…ルール格納ファイル、６…乱数発生ルーチン、７…記憶装置。

代理人　弁理士　鵜沼辰之

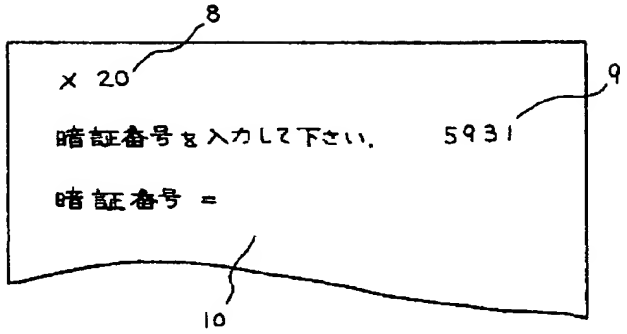
第１図



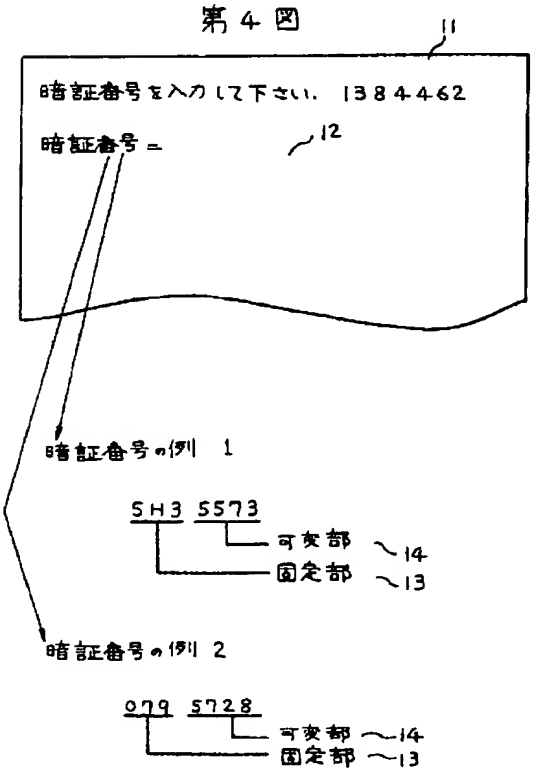
第２図



第３図



第４図



第５図